

AFFIDAVIT IN SUPPORT OF
APPLICATION FOR A SEARCH WARRANT

I, Special Agent (SA) Eric Treglio, upon being duly sworn do hereby state that the following is true to my knowledge and belief:

PRELIMINARY BACKGROUND INFORMATION

1. I am a Special Agent with Homeland Security Investigations (HSI), Department of Homeland Security (DHS) assigned to the Office of the Assistant Special Agent in Charge, Nogales, Arizona. I have been a criminal investigator with Homeland Security Investigations since July 2018. I am a sworn federal law enforcement officer and have authority to investigate federal offenses pursuant to Title 18 of the United States Code. I am currently assigned to the Cyber Crimes Group, which conducts investigations of crimes where computers and the internet are used in the sexual exploitation of children, including (but not limited to) violations of 18 U.S.C. Sections 2252 and 2252A, which prohibit a person from knowingly transporting, receiving, distributing, possessing or accessing with intent to view, in interstate or foreign commerce, or by using any facility or means of interstate or foreign commerce, child pornography, as defined in 18 U.S.C. Section 2256(8). I am a graduate of the Criminal Investigator Training Program and the HSI Special Agent Academy at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia. During the HSI Special Agent Academy, I received formal and on-the-job training in the investigation of cases involving the sexual exploitation of children to include training programs and participation in the execution of search warrants involving child pornography and seizures of computers and other storage media. I have also successfully completed the Internet Crimes Against Children (ICAC) eMule Investigations course held by the National Criminal Justice Training Center.

2. Prior to joining Homeland Security Investigations, I was a United States Border Patrol Agent. I attended the 13 week- federal academy at the Federal Law Enforcement

Training Center in Artesia, New Mexico. I was employed as a United States Border Patrol Agent from 2012 to 2018.

3. The facts set forth in this affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

4. This investigation concerns alleged violations of 18 U.S.C. §§ 2251, 2252, 2252A, and 2422 relating to material involving the sexual exploitation of minors. 18 U.S.C. § 2251(a) prohibits a person from employing, using, persuading, inducing, enticing and coercing a minor to engage in sexually explicit conduct for the purpose of producing a visual depiction of such conduct. 18 U.S.C. §§ 2252 and 2252A prohibit a person from knowingly transporting, receiving, distributing, possessing, or accessing with intent to view, in interstate or foreign commerce, or using any facility or means of interstate or foreign commerce, any visual depictions of minors engaging in sexually explicit conduct (child pornography) as defined in 18 U.S.C. § 2256(8). 18 U.S.C. §§ 2422 prohibits anyone from knowingly persuading, inducing, enticing, or coercing an individual to travel in interstate or foreign commerce with the purpose of engaging in prostitution or any criminal sexual activity, or attempting to do so.

5. This affidavit is offered in support of a search warrant application to search the items described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B. Specifically, as more fully described below, this warrant requests authorization to search one Samsung Galaxy AO3s, Model: SM-A037U,

IME 355819214680849 and one Samsung Galaxy, IME 355019640884558 (hereafter "SUBJECT DEVICES").

6. The SUBJECT DEVICES both are currently in the custody of the HSI office located at 41 Paseo de Yucatan, Rio Rico, AZ, 85648, and have been in said location since their respective seizures.

DEFINITIONS

7. The following non-exhaustive list of definitions applies to this Affidavit and Attachments A and B:

a. Child Pornography is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).

b. Child Erotica means materials or items that are sexually arousing to persons having a sexual interest in minors, but that are not, in and of themselves, obscene or illegal. In contrast to "child pornography," this material does not necessarily depict minors in sexually explicit poses or positions. Some of the more common types of child erotica include photographs that are not sexually explicit, drawings, sketches, fantasy writing, and diaries. *See* Kenneth V. Lanning, *Child Molesters: A Behavioral Analysis* (2001) at 65. Federal courts have recognized the evidentiary value of child erotica and its admissibility in child pornography cases. *See United States v. Cross*, 928 F.2d 1030 (11th Cir. 1991) (testimony about persons deriving sexual satisfaction from and collecting non-sexual photographs of children admissible to show intent and explain actions of defendant); *United States v. Caldwell*, No. 97-5618, 1999 WL 238655 (E.D. Ky. Apr. 13, 1999) (child erotica admissible under Federal Rule of Evidence 404(b) to show knowledge or intent).

c. Visual depictions include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

d. Minor means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

e. Sexually explicit conduct means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. *See* 18 U.S.C. § 2256(2).

f. Computer means an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e)(1).

g. Computer hardware consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices), peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

h. Computer software is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes computer operating systems, applications, and utilities.

i. Computer-related documentation consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software or other related items.

j. Computer passwords and data security devices consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to unlock particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates test keys or hot keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide or booby-trap protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

k. Internet Service Providers or ISPs are commercial organizations, which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone-based dial-up, broadband based access via a digital subscriber line (DSL) or coaxial cable data transmission, dedicated circuits, or satellite-based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name such as a username or screen name, an e-mail address, and an e-mail mailbox and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a coaxial cable system and can access the Internet by using his or her account name and password.

l. ISP Records are records maintained by ISPs pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ISP's servers and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers use. This service by ISPs allows for both temporary and long-term storage of electronic communications and many other types of electronic data and files.

m. Internet Protocol address or IP address refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a subscriber's computer at varying intervals at the discretion of the ISP. IP addresses might also be static meaning an ISP assigns a user's computer a specific IP address which is used each time the computer accesses the Internet.

n. The terms records, documents and materials include all information recorded in any form, visual or aural, and by any means, whether in hand-made form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, printing and/or typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

o. Digital device includes any electronic system or device capable of storing, processing, interpreting or rendering data in digital form, including computer systems of various form factors (computer desktop systems, towers, servers, laptops, notebooks and netbooks), personal digital assistants, cellular telephones and smart phones, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors and drives intended for removable media; related communication devices such as wired and wireless home routers and modems; storage media such as electro-mechanical hard disks, solid state hard disks, hybrid hard disks, floppy disks, optical disks such as compact disks and digital video disks, magnetic tapes and volatile and non-volatile solid state flash memory chips; and security devices including dongles and flash chips.

p. Image or copy refers to an accurate reproduction of information contained on an original physical item, independent of the electronic storage device. Imaging or copying maintains contents, but attributes may change during the reproduction.

q. Hash value refers to a value generated after data has been subjected to a cryptographic mathematical algorithm. A hash value is akin to a digital fingerprint in that dissimilar data will not produce the same hash value after being subjected to the same hash algorithm. Therefore, a hash value is particular to the data from which the hash value was generated. Known hash values can be used to search for identical data stored on various digital devices and/or media as identical data will have the same hash value.

r. Compressed file refers to a file that has been reduced in size through a compression algorithm to save disk space. The act of compressing a file will make it unreadable to most programs until the file is uncompressed.

BACKGROUND ON COMPUTERS AND CHILD EXPLOITATION

8. I have been formally trained in the investigation of crimes involving the sexual exploitation of children. I also own my own computer, have personal knowledge of the operation of a computer, and have accessed the Internet since approximately 1997. Based

on this training and knowledge, and the experience of other law enforcement personnel involved in this investigation, I know the following:

9. The Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across state and national boundaries. Computer technology and the Internet revolutionized the way in which child pornography is produced, distributed, stored, and communicated as a commodity and a further tool of child exploitation. For instance:

a. Individuals can transfer photographs from a camera onto a computer-readable format with a variety of devices, including scanners, memory card readers, or directly from digital cameras, including those on most cellphones.

b. Modems allow computers to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world.

c. The capability of a computer to store images in digital form makes the computer itself an ideal repository for child pornography. As explained further below, the storage capacity of electronic media used in home computers has increased tremendously within the last several years. These drives can store an extreme number of visual images at very high resolution.

d. The Internet, the World Wide Web, and other Internet components afford individuals many different and relatively secure and anonymous venues for obtaining, viewing, and trading child pornography, or for communicating with others to do so or to entice children.

e. Individuals can use online resources to retrieve, store, and share child pornography, including services offered by Internet Service Providers such as Google, Hotmail, America Online (AOL), and Yahoo!, as well as many social media applications which allow chatting, messaging, and sharing of files. Online services allow a user to set

up an account providing e-mail and/or instant messaging services, as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer.

f. As is the case with most digital technology, computer communications and files shared or viewed can be saved or stored on hardware and computer storage media used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite web sites in, for example, bookmarked files. However, digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or footprints in the web cache and history files of the browser used. Such information is often maintained for very long periods of time until overwritten by other data.

g. The interaction between software applications and the computer operating systems often results in material obtained from the Internet being stored multiple times, and even in different locations, on a computer hard drive without the user's knowledge. Even if the computer user is sophisticated and understands this automatic storage of information on his computer's hard drive, attempts at deleting the material often fail because the material may be automatically stored multiple times and in multiple locations within the computer media. As a result, digital data that may have evidentiary value to this investigation could exist in the user's computer media despite, and long after, attempts at deleting it. A thorough search of this media could uncover evidence of production, receipt, distribution, possession, and/or access of child pornography.

h. Data that exists on a computer is particularly resilient to deletion. Computer files or remnants of such files can be recovered months or even years after they have been

downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person deletes a file on a home computer, the data contained in the file does not actually disappear, rather, the data remains on the hard drive until it is overwritten by new data. Therefore, deleted files or remnants of deleted files, may reside in free space or slack space, that is, in space on the hard drive that is not allocated to an active file and is left unused and free to store new data. Such residual data may remain in free space for long periods of time before it is overwritten by new data. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity and computer habits.

i. The interaction between software applications and the computer operating systems often results in material obtained from the Internet being stored multiple times, and even in different locations, on a computer hard drive without the user's knowledge. Even if the computer user is sophisticated and understands this automatic storage of information on his computer's hard drive, attempts at deleting the material often fail because the material may be automatically stored multiple times and in multiple locations within the computer media. As a result, digital data that may have evidentiary value to this investigation could exist in the user's computer media despite, and long after, attempts at deleting it.

**BACKGROUND ON COMPUTERS AND EVIDENCE ASSESSMENT PROCESS
IN CHILD EXPLOITATION INVESTIGATION**

10. This warrant seeks permission to locate not only digital files that might serve as direct evidence of the crimes described in the warrant, but also for evidence that establishes how computing devices were used, the purpose of their use, and who used them.

11. As described above and in Attachment B, this application seeks permission to search and seize certain records that might be found in the SUBJECT DEVICES, in whatever form they are found. One form in which the records might be found is stored on a computer's hard drive, or other electronic media. Some of these electronic records might take the form of files, documents, and other data that is user-generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis. In addition to user-generated documents (such as word processor, picture, and movie files), computer hard drives and storage media can contain other forms of electronic evidence that are not user-generated. In particular, a computer hard drive may contain records of how a computer has been used, the purposes for which it was used and who has used these records, as described further in the attachments.

12. Based upon my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that items to be searched may not only contain child pornography, but also contain the identity of the user/possessor of the child pornography as well as evidence as to the programs and software used to obtain the child pornography. Further, in finding evidence of how a computer has been used, the purposes for which it was used, and who has used it, sometimes it is necessary to establish that a particular thing is not present on a hard drive or that a particular person (in the case of a multi-user computer) was not a user of the computer during the time(s) of the criminal activity. For instance, based upon my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that when a computer has more than one user, files can contain information indicating the dates and times that

files were created as well as the sequence in which they were created, so that evidence of whether a user accessed other information close in time to the file creation dates, times and sequences can help establish user identity and exclude other users from computer usage during relevant times.

13. Because the absence of particular data on a digital device may provide evidence of how a digital device has been used, what it has been used for, and who has used it, analysis of the digital device as a whole may be required to demonstrate the absence of particular data. Such evidence of the absence of particular data on a digital device is not segregable from the digital device.

14. The types of evidence described above may be direct evidence of a crime, indirect evidence of a crime indicating the location of evidence or a space where evidence was once located, contextual evidence identifying a computer user, and contextual evidence excluding a computer user. All of these types of evidence may indicate ownership, knowledge, and intent. This type of evidence is not “data” that can be segregated, that is, this type of data cannot be abstractly reviewed and filtered by a seizing or imaging agent and then transmitted to investigators. Rather, evidence of this type is a conclusion, based on a review of all available facts and the application of knowledge about how a computer behaves and how computers are used. Therefore, contextual information necessary to understand the evidence described in Attachment B also falls within the scope of the warrant.

PROBABLE CAUSE

15. In February 2023, Homeland Security Investigations (HSI), Nogales, Arizona, conducted online undercover chats to proactively target sexual predators that seek to exploit minors via social media, messaging platforms, and through other forms of electronic communication. The goal of the chats was to engage, apprehend, interview, and prosecute targets attempting to sexually exploit minors. During the course of the chats, HSI Special Agents (SA) encountered John BAKER of Tucson, AZ.

On May 10, 2023, HSI Nogales SAs arrested John BAKER, a 69-year-old United States (U.S.) citizen, for Coercion and Enticement of a Minor after he traveled from Tucson, AZ to Sahuarita, AZ where he intended to engage in sexual conduct with a 14-year-old female after months of sexual-in-nature conversation online. Agents arrested BAKER as he drove up to meet the “female minor.” One Samsung Galaxy, IME 355019640884558 phone was seized from BAKER's person. BAKER was booked into the Pima County Detention Facility and prosecution was not accepted by the Pima County Attorney's Office.

On September 6, 2023, John BAKER was indicted by a federal grand jury in the District of Arizona for violation of 18 U.S.C. § 2422(b), Coercion and Enticement of a minor.

16. On October 4, 2023, John BAKER was arrested outside of his home in Tucson, AZ.

17. On October 12, 2023, I was notified by the U.S. Pretrial Services Office that they were contacted by Jennifer Baker. Jennifer Baker is the wife of, and resides with, John BAKER. Jennifer Baker informed Pretrial Services officer's that she had gone through her husband's Samsung Galaxy AO3s IME 355819214680849 after his arrest and found pictures of possible child pornography, otherwise know as Child Sexual Abuse Material (CSAM).

18. On October 13, 2023, HSI SA Bradley Baker traveled to Jennifer and John BAKER's residence at 232 S Placita Aldaco in Tucson, AZ. Jennifer Baker informed SA Baker that she had gone through her husband's cell phone after he was arrested and found numerous pictures of clothed females under the age of eighteen. She also stated that she observed one picture of a completely nude female who was approximately fourteen to fifteen years old in the camera roll or files folder of the phone. Jennifer Baker also stated she found numerous chats with underage females on the phone.

PROCEDURES FOR ELECTRONICALLY STORED INFORMATION
SEARCH METHODOLOGY TO BE EMPLOYED

19. The search methodology to be employed as to computers and digital media is as follows:

a. It is anticipated that mirror copies or images of the SUBJECT DEVICES will be made if failure to do so could otherwise potentially alter the original evidence.

b. Consistent with the information provided within this affidavit, contextual information necessary to understand the evidence, to identify the user/possessor or producer of the child pornography, and to establish admissibility of the evidence in subsequent legal proceedings will also be sought by investigative agents.

c. Additional techniques to be employed in analyzing the seized items will include (1) surveying various file directories and the individual files they contain; (2) opening files to determine their contents; (3) scanning storage areas, (4) performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in this affidavit and its attachments, and (5) performing any other data analysis techniques that may be necessary to locate and retrieve the evidence described in this affidavit and its attachments.

d. Because it is expected that the SUBJECT DEVICES may constitute (1) an instrumentality of the offense, (2) fruit of criminal activity, (3) contraband, or (4) evidence otherwise unlawfully possessed, it is anticipated that such evidence will not be returned to the owner and that it will be either forfeited or ultimately destroyed in accordance with the law at the conclusion of the case. However, if after careful inspection investigators determine that such devices do not contain (1) instrumentality of the offense, (2) fruit of criminal activity, (3) contraband, (4) evidence otherwise unlawfully possessed, or (5) evidence of the person who committed the offense and under what circumstances the offense was committed, then such items seized will be returned.

20. Following the issuance of this warrant, HSI Agents will collect the SUBJECT DEVICES and subject them to analysis. All forensic analysis of the data contained within the DEVICES will employ search protocols directed exclusively to the identification and extraction of data within the scope of this warrant. Based on the foregoing, identifying, and extracting data subject to seizure pursuant to this warrant may require a range of data analysis techniques, including manual review, and, consequently, may take weeks or months.

RETURN AND REVIEW PROCEDURES

21. Pursuant to Rule 41 of the Federal Rules of Criminal Procedure, I understand and will act in accordance with the following:

a. Pursuant to Rule 41(e)(2)(A)(i), an agent is required to file with the court an inventory return, that is, an itemized list of the property seized, within fourteen (14) days of the execution of the warrant.

b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within which the electronically stored information must be seized or copied on-site after the issuance of the warrant, not the later review of the media or information seized, or the later off-site digital copying of that media.

c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court may be limited to a description of the physical storage media that was seized or copied, not an itemization of the information or data stored on the physical storage media. Under Rule 41(f)(1)(B), I may retain a copy of that information for purposes of the investigation. The government intends to make and retain a full image copy of the seized media, so that a copy of the evidence, rather than the original evidence, can be examined. The government will seize and retain both the original evidence and any copies of this evidence. This procedure will ensure that the original evidence remains intact and that potential child pornography and instrumentalities of such crime will not be returned to the subject.

CONCLUSION

22. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of such criminal offenses may be located on items described in Attachment A, in violation of 18 U.S.C. §§ 2251, 2252, 2252A, and 2422. I therefore respectfully request that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

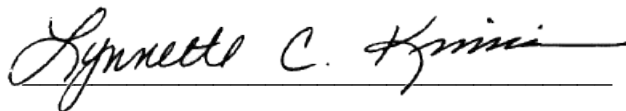
ERIC M
TREGLIO

Digitally signed by ERIC M
TREGLIO
Date: 2023.10.19 13:51:09
-07'00'

Eric Treglio, Special Agent

Homeland Security Investigations

SUBSCRIBED and SWORN to telephonically before me
this 19th day of October 2023



HON. LYNNETTE C. KIMMINS

UNITED STATES MAGISTRATE JUDGE